

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

KAREN PEKELNEY and MARK MEISEL, on
behalf of themselves and all others similarly
situated,

Plaintiffs,

v.

HORIZON HEALTHCARE SERVICES, INC.,
d/b/a HORIZON BLUE CROSS BLUE
SHIELD OF NEW JERSEY, a New Jersey
corporation;

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Karen Pekelney (“Plaintiff Wife”) and Mark Meisel (“Plaintiff Husband”) individually and on behalf of all others similarly situated, bring this class action against HORIZON HEALTHCARE SERVICES, INC., d/b/a HORIZON BLUE CROSS BLUE SHIELD OF NEW JERSEY (“Defendant” or “Horizon”), and allege upon personal knowledge as to themselves and upon information and belief as to the other allegations of this Complaint, as follows:

INTRODUCTION

1. This nationwide class action is brought by Plaintiff Wife and Plaintiff Husband (collectively “Plaintiffs”) against Defendant for failing to adequately secure and safeguard its members’ (1) sensitive personally identifiable information (“PII”), which includes without limitation members’ names, dates of birth, Social Security numbers, and addresses; and (2) protected health information (“PHI”) which contains PII, in addition to members’ demographic

information, medical histories, test and laboratory results, insurance information, and other data collected by health care professionals to identify an individual and determine appropriate care.

2. In early November 2013, two unencrypted laptop computers were stolen from Defendant's headquarters in Newark, New Jersey. In December 2013, Defendant sent letters to Plaintiff Wife and Plaintiff Husband alerting them that the stolen laptops may have contained their PII and PHI. According to Defendant's website, over 839,000 members were being notified in a similar fashion.

3. In its Privacy Policy, Defendant falsely claims that it "maintain[s] appropriate administrative, technical and physical safeguards to reasonably protect [members'] Private Information."

4. The 2013 massive data breach could have been prevented. Six years earlier, in early January 2008, Horizon suffered a similar theft, placing it on notice of the vulnerability of its data security. At that time, a different laptop containing PII for roughly 300,000 members was stolen from the residence of one of Defendant's employees. The massive breach caught the attention of government officials, prompting an inquiry into Defendant's practices. Defendant responded by claiming to be in the process of encrypting all desktops, laptops, and portable media devices, a process it anticipated would be completed in March 2008.¹

5. Apparently Defendant ignored the warnings of government officials in 2008: The laptops stolen in 2013 contained members' unencrypted PII as well as PHI. Defendant's failure to comply with longstanding industry standard encryption protocols was a violation of its own privacy practices and jeopardized Defendant's members' PII and PHI.

¹ *Insurer gives lawmakers reassurance of patient-data security*, Press of Atlantic City (New Jersey), Feb. 20, 2008.

6. Because of the 2008 laptop theft and ensuing public concern, Defendant assuredly knew the risks involved in maintaining sensitive member PII and PHI on unencrypted laptops and indeed publicly stated it would change its practices; nonetheless, Defendant continued to store such sensitive material in an unsafe manner.

7. Plaintiffs bring this lawsuit on behalf of themselves and all others in the United States who enrolled in Defendant's health insurance plans on or before November 3, 2013, and whose PII or PHI resided on one or more laptops stolen from Defendant's headquarters in Newark on or about November 1-3, 2013, alleging that Defendant has violated the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681 – 1681x, the New Jersey Consumer Fraud Act, breached its contract with Plaintiffs and members of the proposed Class, and acted negligently in safeguarding its members' PII and PHI. Plaintiffs seek damages as well as injunctive relief requiring Defendant to take steps to ensure that its members' PHI and PII are adequately protected.

PARTIES

8. Plaintiff Wife, a citizen and resident of New Jersey, has been a member of a health insurance plan offered by Defendant since 2011. Plaintiff Wife received a letter from Defendant in December 2013 notifying her that two unencrypted laptops stolen from Defendant's headquarters may have contained her PII and PHI. Plaintiff Wife has sustained, and continues to sustain, damages as a result.

9. Plaintiff Husband, a citizen and resident of New Jersey, was a member of a health insurance plan offered by Defendant from 2011 through in or about October 2012. Plaintiff Husband received a letter from Defendant in December 2013 notifying him that two unencrypted

laptops stolen from Defendant's headquarters may have contained his PII and PHI. Plaintiff Husband has sustained, and continues to sustain, damages as a result.

10. Defendant Horizon Healthcare Services, Inc., d/b/a Horizon Blue Cross Blue Shield of New Jersey is a health service corporation headquartered in Newark, New Jersey.²

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiffs' FCRA claims pursuant to 28 U.S.C. § 1331 and their state law claim pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendant because Defendant is headquartered in New Jersey and at all relevant times conducted substantial business in the District of New Jersey.

13. Venue is proper in the District of New Jersey under 28 U.S.C. § 1391 because Defendant resides in this District, and a substantial part of the events giving rise to the claims alleged in this Complaint took place in this District.

FACTUAL ALLEGATIONS

Defendant's Collection of Data

14. When individuals enroll in one of Defendant's health plans, they fill out an enrollment form.

15. Defendant's enrollment form requires a prospective member to provide a variety of sensitive information, including one's full name, Social Security number, date of birth, sex, full address, home phone, e-mail address, alternative addresses, one's race or ethnicity, the name and address of one's primary care provider, any preexisting conditions, and information regarding coverage under other health insurance plans.

² *Fast Facts*, HorizonBlue.com <http://www.horizonblue.com/about-us/our-company/company-information/fast-facts> (last visited Jan. 21, 2014).

16. Defendant's enrollment form thus requires a prospective member to provide Defendant with the prospective member's PII and PHI.

17. Defendant's enrollment form also require a prospective member to provide the information listed in ¶ 15 for other covered members, such as the prospective member's spouse, domestic partner, or children.

18. Defendant's enrollment form may require a prospective member to provide Defendant with PII and PHI for a prospective member's spouse, domestic partner, or children.

19. When Plaintiffs enrolled in Defendant's health plan, they completed one or more enrollment forms in which they provided Defendant with their PII and PHI, including their full names, addresses, dates of birth, and Social Security numbers.

20. When members file claims (or when claims are filed on members' behalf), additional PHI or PII is transmitted to Defendant.

21. Roughly 3.7 million members are enrolled in Defendant's health insurance plans.³

Defendant's Reassurances of Adequate Security

22. On its website, Defendant states:

Our employees are trained on the need to maintain your Private Information in the strictest confidence. They agree to be bound by that promise of confidentiality and are subject to disciplinary action if they violate that promise. We also maintain appropriate administrative, technical and physical safeguards to reasonably protect your Private Information.

In addition, in those situations where we rely on a third party to perform business, professional or insurance services or functions for us, that third party must agree to safeguard your Private Information. That business associate must also agree to use it only as required to perform its functions for us and as otherwise permitted by our contract and the law. Finally, if we or our business associate causes a "breach" of privacy as that term is

³ *Id.*

defined under federal law, we will notify you without unreasonable delay of the occurrence. In these ways, we carry out our confidentiality commitments to you.

How Defendant Uses the Data it Collects

23. Defendant shares PII, PHI, and other information with a variety of third parties, including suppliers, vendors, health care providers, pharmacies, board members, and other entities.

24. According to Defendant's Privacy Policy, Defendant may use and disclose members' PII, PHI, or both for a variety of purposes, including without limitation: (1) payment activities; (2) health care operations activities; (3) health-related activities; (4) treatment, payment and health care operations of other covered entities; (5) public health activities; (6) health oversight agencies; (7) to carry out appropriate research; (8) to contact members for fundraising purposes; (9) to conduct marketing activities; and (10) to perform other functions and activities permitted by the federal privacy rules.

The First Theft: 2008

25. Defendant claims to maintain appropriate administrative, technical and physical safeguards to reasonably protect its members' Private Information.

26. In early January 2008, a laptop containing PII for roughly 300,000 members was stolen from the residence of one of Defendant's employees. At that time, Defendant stated that the laptop had a special security feature: it was programmed to automatically destroy the PII on January 23, 2008.⁴

27. Following the 2008 theft, state legislators requested that the New Jersey Attorney General and the United States Attorney for the District of New Jersey investigate Defendant,

⁴ *Laptop Stolen containing data on 300,000 customers of Horizon Blue Cross/Blue Shield*, <http://www.givemebackmycredit.com/blog/2008/02/laptop-stolen-containing-data.html> (last visited Jan. 27, 2014)

noting that “Horizon is one of the state’s largest health insurance companies and the major provider of benefits for public employees, many of whom are retired and have moved out of state. . . . It is outrageous that such a security breach could happen, and its repercussions could certainly cross state lines.”⁵

28. In response to public concerns about its data protection policies, Defendant stated that it had begun encrypting all desktops, laptops, and portable media devices, a process it anticipated would be completed in March 2008.⁶

29. A September 2008 news article indicated that a spokesman for Defendant had stated that Defendant had taken steps to improve security and was requiring that all computers be fully encrypted.⁷

The Second Theft: 2013

30. Sometime during the weekend of November 1-3, 2013, two laptop computers were stolen from Defendant’s headquarters in Newark, New Jersey.

31. The stolen laptops had been merely “cable-locked” to employee workstations; cable-locks are easily defeated with common items including office supplies, soda cans, and toilet paper rolls.⁸

⁵ *Assemblyman Chiusano Says Massive Horizon Identity Theft Warrants State, Federal Investigations*, US States News, Jan. 30, 2008.

⁶ *Insurer gives lawmakers reassurance of patient-data security*, Press of Atlantic City (New Jersey), Feb. 20, 2008.

⁷ *When sensitive data is lost; Companies taking steps to combat rising problem of security breaches*, The Record (Bergen County, NJ), Sept. 3, 2008.

⁸ *Blue Cross: 840,000 healthcare records at risk after laptop theft*, <http://www.networkworld.com/news/2013/121013-blue-cross-840000-healthcare-records-276801.html> (last visited Jan. 24, 2014).

32. The stolen laptops were password-protected; however, passwords are easily defeated, and only encryption can protect PII or PHI on a laptop.⁹

33. The data on the laptops stolen the weekend of November 1-3, 2013 was not encrypted.

34. Defendant discovered the theft of the laptops on or about November 4, 2013.

35. Horizon publicly announced that the stolen laptops may have contained PII, PHI, or both types of information for as many as 839,700 current or former members of Defendant's health plans.

36. Even though Defendant's security policy promises consumers it will "notify you without unreasonable delay" of a breach of security, it delayed notification to its members for more than one month.

37. It was not until December 6, 2013, that Defendant publicly announced on its website the theft of its laptops containing members' unencrypted PII and PHI:

[T]wo password-protected, unencrypted laptop computers that were cable-locked to employee workstations were stolen from [our] Newark headquarters during the weekend of November 1, 2013.

A detailed review led by outside computer forensic experts has confirmed that the laptops may have contained files with differing amounts of member information, including name and demographic information (e.g., address, member identification number, date of birth), and in some instances, a Social Security number and/or limited clinical information. Due to the way the stolen laptops

⁹ American Medical Association, *HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information*, <http://www.ama-assn.org/resources/doc/washington/hipaa-phi-encryption.pdf>.

were configured, it is not certain that all of the member information contained on the laptops is accessible.¹⁰

38. Plaintiffs each received a December 6, 2013, letter from Defendant stating:

Horizon BCBSNJ also began an internal investigation to determine what information was contained on the stolen laptops. Working with outside computer forensic experts, we have confirmed that the laptops may have contained your name, Social Security number, and demographic information (e.g., address, date of birth, Horizon BCBSNJ identification number). Due to the way the stolen laptops were configured, we are not certain that all of this information is accessible.

39. Defendant employed fewer security features in 2013 than in 2008: Defendant's December 6, 2013, letters to Plaintiffs did *not* state that the laptops stolen in 2013 were programmed to automatically destroy the information on them by a certain date.

40. Plaintiff Husband has not been a member of any of Defendant's health plans since on or about October 31, 2012, and any claims that he submitted pursuant to his former health plan with Defendant were submitted and fully paid prior to November 1, 2012.

41. Even though Plaintiff Husband had not been a member in any of Defendant's health plans for at least a year prior to the theft, his PII and PHI were stored in an unencrypted fashion on the laptops stolen in November 2013.

42. According to Defendant's website, Defendant allegedly notified more than 839,000 current or former members that their PII and PHI may have been contained on the laptops stolen in November 2013.

43. Defendant offered Plaintiffs and others affected by the theft a free, one-year membership in Experian's ProtectMyID Alert which is insufficient given that it can take years to resolve instances of identity theft.¹¹

¹⁰ *Horizon Blue Cross Blue Shield of New Jersey Notifies Members, Offers Protection Following Office Theft*, <http://www.horizonblue.com/about-us/news-overview/company-news/horizon-bcbsnj-notifies-members> (last visited Jan. 26, 2014).

44. According to the ProtectMyID website, although ProtectMyID will check a consumer's credit report on a daily basis for new accounts and other reportable transactions, it does not monitor misuse of existing financial accounts or medical identity unless such misuse results in a new loan or other transaction that would appear on a credit report. As a result, ProtectMyID may not detect all misuse of a consumer's PII or PHI, or it may detect the misuse well after significant harm has occurred.

45. PHI may contain information about a consumer's personal life, such as lifestyle, fitness, diseases, and possibly genetic information, all of which could be used to impersonate victims or possibly blackmail individuals in public positions; ProtectMyID does not protect against such harms.¹²

46. On January 27, 2014, several of Defendant's high-ranking executives testified before the New Jersey Senate Health, Human Services and Senior Citizens Committee. At that hearing, Sen. Joseph Vitale stated he had consulted with information security experts who stated that the protection of the data on the laptops was "very sloppy." Sen. Vitale also questioned the length of the credit protection services offered by Defendant.

47. At the January 27, 2014 hearing before the New Jersey Senate Health, Human Services and Senior Citizens Committee, Defendant confirmed that it had not encrypted all of its computers.

¹¹ *Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen*, <http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/> (last visited Jan. 27, 2014).

¹² *Healthcare Data of 840,000 at Risk After Laptop Theft*, <http://mashable.com/2013/12/19/horizon-blue-cross-blue-shield-laptop-theft/> (last visited Jan. 26, 2014).

48. Nearly six years after the first security breach, Defendant essentially admitted it had not taken the steps it had promised to take in 2008 to improve the security of its members' PII and PHI, such as encrypting all of its computers. Instead, Defendant stated to members in its December 2013 letter:

To help prevent something like this from happening in the future, we are strengthening our encryption processes and enhancing our policies, procedures and staff education regarding the safeguarding of company property and member information. Be assured that protecting your information is a priority at Horizon BCBSNJ.

49. According to the press, Defendant still does not know the location of the stolen laptops.

CLASS ACTION ALLEGATIONS

50. Plaintiffs bring this action on behalf of themselves and a class of persons initially defined as follows:

All persons in the United States who enrolled in any of Defendant's health insurance plans on or before November 1, 2013 and whose PII or PHI resided on one or more laptops stolen from Defendants' headquarters in Newark, New Jersey on or about November 1-3, 2013.

51. Excluded from the Class are Defendant; any affiliate, parent or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any officer, director or employee of Defendant; any successor or assign of Defendant; anyone employed by counsel for Plaintiffs in this action; any Judge to whom this case is assigned as well as his or her immediate family and staff.

52. This action has been brought and may properly be maintained on behalf of the Class proposed above under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

53. Numerosity. Members of the Class are so numerous that their individual joinder herein is impracticable. Defendant has stated that it was alerting 839,000 members that their PII or PHI may have been on one or more of the stolen, unencrypted laptops.

54. Existence and predominance of common questions. Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual Class members. These common questions include the following:

- a) Whether Defendant violated FCRA by failing to encrypt or otherwise adequately protect members' PII and PHI;
- b) Whether Defendant was negligent in how it stored and maintained members' PII and PHI;
- c) Whether Defendant had a duty to protect its members PII and PHI;
- d) Whether Defendant breached its duty to protect its members PII and PHI; and
- e) Whether Plaintiffs and Class members sustained damages resulting from Defendant's failure to protect its members PII and PHI.

55. Typicality. Plaintiffs' claims are typical of the claims of the Class because the claims of Plaintiffs and all Class members arise from the same set of facts regarding Defendant's failure to protect Class members' PII and PHI.

56. Adequacy. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class they seek to represent. Plaintiffs have retained counsel competent and experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

57. Superiority. The class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class member is not of such magnitude as to make the prosecution of individual actions against Defendant economically feasible. Even if Class members themselves could afford such individualized litigation, the court system could not. In addition to the burden and expense of managing myriad actions arising from the alleged misrepresentations, individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

58. In the alternative, the Class may be certified because Defendant has acted on grounds generally applicable to the Class, thereby making appropriate injunctive relief with respect to the members of the Class as a whole;

59. The prosecution of separate actions by the individual member of the Class would create a risk of inconsistent or varying adjudications with respect to individual Class members which would establish incompatible standards of conduct for Defendant; and

60. The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests.

FIRST CAUSE OF ACTION

(For willful violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681n(a))

61. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

62. Defendant's acts and practices, as alleged in this complaint, constitute a willful violation of FCRA, 15 U.S.C. § 1681n(a), which provides that "[a]ny person who willfully fails to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of . . . any actual damages sustained by the consumer as a result of the failure or damages of not less than \$100 and not more than \$1,000" in addition to punitive damages, costs, and attorney's fees.

63. In enacting FCRA, Congress found that "[c]onsumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers" and "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy." 15 U.S.C. § 1681(a).

64. FCRA requires that "consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter." 15 U.S.C. § 1681(b).

65. Under FCRA, a "consumer reporting agency" is "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on

consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” 15 U.S.C. § 1681a(f).

66. Under FCRA, a “consumer report” is “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for—(A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title.” 15 U.S.C. § 1681a(d).

67. Pursuant to 15 U.S.C. § 1681b, a “consumer reporting agency may furnish a consumer report . . . [t]o a person which it has reason to believe . . . intends to use the information in connection with the underwriting of insurance involving the consumer.”

68. Defendant’s privacy policy states:

We routinely use and disclose Private Information in connection with your health care coverage, to determine your eligibility for coverage and benefits, and to see that the treatment and services you receive are properly billed and paid. To do this, we may share Private Information with health care providers, their billing agents, insurance companies and others. Our payment activities can also include the use of Private Information for: risk adjustment, billing, claims management, collection activities, utilization review, medical necessity determinations, drug rebate contract reporting of drug utilization, underwriting and other rate-setting activities.

69. Defendant is a consumer reporting agency under FCRA:

a) Member PII and PHI consists of information on consumers;

- b) Defendant regularly engages in assembling or evaluating PII and PHI to furnish consumer reports to the third parties listed in ¶¶ 23-24 and 68; and
- c) Defendant uses mail, e-mail, or other means of interstate commerce to prepare or furnish PII and PHI to the third parties listed in ¶¶ 23-24 and 68.

70. Defendant furnishes consumer reports under FCRA as follows:

- a) Defendant provides PII and PHI to the third parties listed in ¶¶ 23-24 and 68;
- b) PII and PHI bear on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living; and
- c) Defendant provides PII and PHI to the third parties listed in ¶¶ 23-24 and 68 to serve as a factor in:
 - a. establishing members' eligibility for insurance; or
 - b. underwriting insurance for its members.

71. Defendant is part of a national network of roughly 38 health plans that serve in total nearly 100 million persons in the United States.¹³

72. Providers of health insurance within the national network referenced in ¶ 71 may make an explicit FCRA disclosure in their enrollment forms.

73. For example, Arkansas Blue Cross and Blue Shield is also part of national network referenced in ¶ 71.

¹³ *Fast Facts*, HorizonBlue.com <http://www.horizonblue.com/about-us/our-company/company-information/fast-facts> (last visited Jan. 21, 2014).

74. Arkansas Blue Cross and Blue Shield's "Individual/Family Health Insurance Underwriting Change Form" contains the following notice:

Fair Credit Reporting Act Notice — Notice to Proposed Insured

In connection with your application for insurance, an investigative consumer report may be prepared. Information may be obtained through personal interviews with your family, friends, neighbors, business associates, financial sources, or others with whom you are acquainted. This inquiry includes information as to your character and general reputation. If an investigative consumer report is prepared in connection with your application, you may receive a copy of that report upon written request to Arkansas Blue Cross and Blue Shield. Your written request should be forwarded to Arkansas Blue Cross and Blue Shield, Individual Underwriting Division, P.O. Box 2181, Little Rock, Arkansas 72203-2181.¹⁴

75. Defendant failed to adopt reasonable procedures for maintaining the confidentiality of members' PII and PHI.

76. In light of the 2008 laptop theft and Defendant's ensuing assurances that it would encrypt *all* laptops, Defendant's failure to encrypt or otherwise adequately protect the confidentiality of members' PII and PHI was *willful*, in violation of 15 U.S.C. § 1681(b).

77. As a result of Defendant's violation of 15 U.S.C. § 1681(b), Plaintiffs and the Class are entitled to relief under 15 U.S.C. § 1681n(a) of (i) statutory damages of not less than \$100 and not more than \$1,000 each; (ii) punitive damages; (iii) costs; and (iv) attorney's fees.

SECOND CAUSE OF ACTION

(For negligent violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681n(a))

78. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

¹⁴ Individual/Family Health Insurance Underwriting Change Form, [http://www.arkansasbluecross.com/doclib/forms/members/undchg_form_\(r07-12\).pdf](http://www.arkansasbluecross.com/doclib/forms/members/undchg_form_(r07-12).pdf).

79. Defendant's acts and practices, as alleged in this complaint, constitute a negligent violation of FCRA, 15 U.S.C. § 1681o, which provides that "[a]ny person who is negligent in failing to comply with any requirement imposed under this subchapter with respect to any consumer is liable to that consumer in an amount equal to the sum of—(1) any actual damages sustained by the consumer as a result of the failure; and (2) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court."

80. Defendant failed to adopt reasonable procedures for maintaining the confidentiality of members' PII and PHI.

81. In light of the 2008 laptop theft and Defendant's ensuing assurances that it would encrypt *all* laptops, Defendant's failure to encrypt or otherwise adequately protect the confidentiality of members' PII and PHI was *negligent*, in violation of 15 U.S.C. § 1681(b).

82. Defendant's failure to remove the PII and PHI of former members of Defendant's health plans for whom no claims were pending was *negligent*, in violation of 15 U.S.C. § 1681(b).

83. As a result of Defendant's violation of 15 U.S.C. § 1681(b), Plaintiffs and the Class are entitled to relief under 15 U.S.C. § 1681o of (i) actual damages; (ii) costs; and (iii) attorney's fees.

THIRD CAUSE OF ACTION

(Negligence)

84. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

85. Defendant had a duty to exercise reasonable care to protect and secure Plaintiffs' and the proposed Class members' PII and PHI within its possession or control.

86. Through its acts and omissions, Defendant violated its duty to use reasonable care to protect and secure Plaintiffs' and the proposed Class members' PII and PHI within its possession or control.

87. Defendant negligently failed to encrypt or otherwise electronically protect and secure Plaintiffs' and the proposed Class members' PII and PHI within its possession or control, allowing an unauthorized third-party to possess and control Plaintiffs' and the proposed Class members' PII and PHI.

88. Defendant negligently failed to physically protect and secure Plaintiffs' and the proposed Class members' PII and PHI within its possession or control, allowing an unauthorized third-party to possess and control Plaintiffs' and the proposed Class members' PII and PHI.

89. Defendant negligently retained Plaintiffs' and the proposed Class members' PII and PHI longer than was reasonably necessary.

90. As a direct and proximate result of Defendant's breach of its duties, an unauthorized third-party gained possession and control of the PII and PHI, causing harm to Plaintiffs and the proposed Class by placing them at an increased risk of identity theft, blackmail, and related financial harms. Plaintiffs and the proposed Class have spent, and will continue to have to spend, a significant amount of time and money to protect themselves, their credit, and their reputation as a result of Defendant's conduct.

FOURTH CAUSE OF ACTION

(Breach of Contract)

91. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

92. Defendant came into possession of Plaintiffs' and the proposed Class members' PII and PHI for the purposes of providing and administering health insurance plans and related services to Plaintiffs and the proposed Class.

93. Upon information and belief, the health insurance contract and associated handbook either explicitly or implicitly required Defendant to safeguard and protect Plaintiffs' and the proposed Class members' PII and PHI.

94. Plaintiffs and the proposed Class members were either parties to or third-party beneficiaries of the contract.

95. As consideration under the contract, Plaintiffs and the proposed Class members paid regular premiums, amounting to thousands of dollars paid by each plan member per year.

96. Plaintiffs and the proposed Class members would not have been willing to each pay thousands of dollars per year had they known that their PII and PHI would be stolen, possessed, or controlled by unauthorized third-parties.

97. Defendant did not safeguard or protect Plaintiffs' and the proposed Class members' PII and PHI from being stolen, possessed, or controlled by an unauthorized third-party.

98. Because Defendant failed to safeguard and protect Plaintiffs' and the proposed Class members' PII and PHI, Defendant breached its contract with Plaintiffs and the proposed Class members, reducing the value of the health insurance plans they purchased from Defendant

and causing Plaintiffs and the proposed Class members to suffer, and continue to suffer, actual damages.

FIFTH CAUSE OF ACTION

(Misrepresentation or Omission in Violation of the New Jersey Consumer Fraud

Act, N.J.S.A. §§ 56:8-2 *et seq.*)

99. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

100. The New Jersey Consumer Fraud Act defines merchandise as “any objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale.” N.J.S.A. § 56.8-1(c).

101. The health insurance plans sold by Defendant to Plaintiffs and members of the proposed Class constitute merchandise under the New Jersey Consumer Fraud Act.

102. Under the New Jersey Consumer Fraud Act, the following qualifies as an unlawful practice:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.

N.J.S.A. § 56:8-2.

103. In enacting the New Jersey Consumer Fraud Act, the New Jersey Legislature found that “[i]dentity theft is an act that violates the privacy of our citizens and ruins their good names:

victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories.” N.J.S.A. § 56:11-45(d).

104. As a result of the misrepresentations and omissions set forth in ¶¶ 105 – 113 below, Plaintiffs and the proposed Class members suffered and will continue to suffer an ascertainable loss, damages, and treble damages pursuant to N.J.S.A. § 56:8-19, including without limitation the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, medical fraud, loss of privacy, blackmail, and other economic and non-economic harm.

Misrepresentation

105. Defendant’s 2008 public promise to encrypt all computers and privacy policy promising to protect members’ PII and PHI constitute an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation because Defendant knew that it had not encrypted all of its computers and had not adopted other adequate electronic or physical safeguards to safeguard its members’ PII and PHI.

106. Defendant’s 2008 public promise to encrypt all computers and privacy policy promising to protect members’ PII and PHI constitute an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation in violation of N.J.S.A. § 56:8-2.

Omission

107. Defendant did not tell Plaintiffs and the members of the proposed Class that it had not encrypted all computers and that its data security was inadequate, constituting concealment, suppression, or omission of a material fact.

108. Defendant intended for Plaintiffs and the members of the proposed Class to rely upon the concealment, suppression, or omission of material fact relating to its data security when they entered into or renewed their health insurance contracts with Defendant.

109. In 2008, Defendant provided health insurance to roughly 3.3 million members.¹⁵

110. As stated in ¶ 21, Defendant provides health insurance to roughly 3.7 million members today.

111. Membership in Defendant's health insurance plans would not have increased by over 10% from 2008 if Defendants had not concealed, suppressed, or omitted the material fact relating to its data security.

112. Plaintiffs and the members of the proposed Class would not have enrolled or renewed their health insurance contracts with Defendant if Defendants had not concealed, suppressed, or omitted the material fact relating to Defendant's data security.

113. Defendant's actions constitute a knowing, concealment, suppression, or omission of material fact with intent that others rely upon such concealment, suppression, or omission in violation of N.J.S.A. § 56:8-2.

SIXTH CAUSE OF ACTION

(Failure to Destroy Unneeded Records in Violation of the New Jersey Consumer Fraud

Act, N.J.S.A. § 56:8-2 et seq.)

114. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

¹⁵ *Sen. O'Toole Calls for Hearings, Investigation of Massive Data Loss by Horizon Blue Cross/Blue Shield*, US States News, Jan. 30, 2008.

115. The New Jersey Consumer Fraud Act provides that it is “an unlawful practice and a violation of P.L.1960, c. 39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate” Sections §§ 56:8-161-164 of that Act.

116. Section 56:8-162 of the New Jersey Consumer Fraud Act requires that a business “destroy, or arrange for the destruction of, a customer’s records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means.” N.J.S.A. § 56:8-162.

117. Defendant’s retention of Plaintiffs’ and the proposed Class members’ PII and PHI well after members were no longer covered under Defendant’s health plans violated N.J.S.A. § 56:8-162.

118. As a result of the foregoing, Plaintiffs and the proposed Class members suffered and will continue to suffer an ascertainable loss, damages, and treble damages pursuant to N.J.S.A. § 56:8-19, including without limitation the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, medical fraud, loss of privacy, blackmail, and other economic and non-economic harm.

SEVENTH CAUSE OF ACTION

(Failure to Expediently Notify Following Security Breach in Violation of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-2 et seq.)

119. Plaintiffs, on behalf of themselves and all others similarly situated, reallege as if fully set forth, each and every allegation set forth in this Complaint.

120. The New Jersey Consumer Fraud Act provides that it is “an unlawful practice and a violation of P.L.1960, c. 39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate” Sections §§ 56.8-161-164 of that Act.

121. Section 56:8-163 of the New Jersey Consumer Fraud Act requires that a business conducting business in New Jersey “shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.” N.J.S.A. § 56:8-163

122. The New Jersey Consumer Fraud Act defines a breach of security as follows:

“Breach of security” means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable. Good faith acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56.8-161.

123. The 2013 theft of the laptops from Defendant’s headquarters constituted a breach of security.

124. Defendant's disclosure regarding the breach of security to Plaintiffs and the proposed Class was delayed and therefore not made in the most expedient time possible in violation of N.J.S.A. § 56:8-163.

125. As a result of the foregoing, Plaintiffs and the proposed Class members suffered and will continue to suffer an ascertainable loss, damages, and treble damages pursuant to N.J.S.A. § 56:8-19, including without limitation the cost and time spent on bank and credit monitoring, identity theft, insurance fraud, medical fraud, loss of privacy, blackmail, and other economic and non-economic harm.

PRAYER

WHEREFORE, Plaintiffs, on Plaintiffs' own behalf and on behalf of the Class, pray for judgment as follows:

- a. For an order certifying the Class and appointing Plaintiffs and their counsel to represent the Class;
- b. For an order requiring Defendant to take steps to ensure that its members' PHI and PII is adequately protected;
- c. For an order awarding Plaintiffs and the other Class members statutory, actual, and punitive damages;
- d. For an order enjoining Defendant from continuing to store PII and PHI in an unencrypted manner;
- e. For an order awarding Plaintiffs and Class members pre-judgment and post judgment interest;
- f. For an order awarding Plaintiffs and Class members reasonable attorneys' fees and costs of suit, including expert witness fees; and

- g. For an order awarding such other and further relief as this Court may deem just and proper.

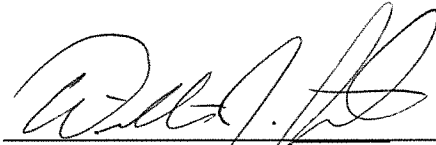
DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable as a matter of right.

DATED: January 28, 2014

Respectfully submitted,

By:



William J. Pinilis (WJP2130)
KAPLAN FOX & KILSHEIMER LLP
160 Morris Street
Morristown, NJ 07960
Telephone: (973) 656-0222
Facsimile: (973) 401-1114
wpinilis@kaplanfox.com

Robert N. Kaplan
David A. Straite (DS6793)
Lauren I. Dubick
KAPLAN FOX & KILSHEIMER LLP
850 3rd Avenue, 14th Floor
New York, New York 10022
Telephone: (212) 687-1980
Facsimile: (212) 687-7714
rkaplan@kaplanfox.com
dstraite@kaplanfox.com
ldubick@kaplanfox.com

Laurence D. King
Linda M. Fong
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
lking@kaplanfox.com
lfong@kaplanfox.com

Attorneys for Plaintiffs